PLANET
Networking & Communication

802.11g Wireless USB 2.0 Adapter

WL-U356

User's Manual

Copyright

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules.   These limits are designed to provide reasonable protection against harmful interference in a residential installation.   This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.   However, there is no guarantee that interference will not occur in a particular installation.   If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1.   Reorient or relocate the receiving antenna.
2.   Increase the separation between the equipment and receiver.
3.   Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4.   Consult the dealer or an experienced radio technician for help.

FCC Caution:

To assure continued compliance.(example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Not Intended for Use

The ETSI version of this device is intended for home and office use in Austria Belgium, Denmark, Finland, France (with 4 Frequency channel restrictions). Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain (with 2 Frequency channel restrictions), Sweden and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

Revision

User's Manual for PLANET Wireless USB Adapter

Model: WL-U356

Rev: 1.0 (June. 2004)

Part No. EM-WLU356

TABLE OF CONTENTS

Chapter 1 Introduction

Complying with the IEEE 802.11g standard, WL-U356 provides simple, reliable, high-speed wireless connectivity for both desktop and laptop users. By combining two, state-of-the-art technologies—USB 2.0 and 802.11g—the gadget delivers data at speed up to 54Mbps, five times the speed of existing 802.11b devices, and spares the effort of opening up the case of your desktop computer.

WL-U356 contains an internal patch antenna. It takes advantage of the flexibility and convenience of USB connections without sacrificing performance. Support of 64, 128 and 256-bit WEP encryption plus WPA (Wi-Fi Protected Access) high-level encryption prevents your wireless communications from unauthorized access and ensures secure data transfer.

WL-U356 supports software AP function, which can turn the USB adapter into a compact Access Point instantly. The USB adapter is also backward compatible with 802.11b products, so both 11b and 11g clients can reside on the same network. Easy installation and Hot-plugging offers full mobility and high availability, making the device a perfect choice for users who are getting tired of running cables or in constant need of wireless access.

1.1 Features

- 2.4GHz ISM band, unlicensed operation
- Wireless connectivity without the hassles and cost of running cables
- IEEE 802.11b/g standard compliant
- USB 2.0 A-type standard connector, compatible with USB 1.1
- Up to 54Mbps data rate
- Utilization of Direct Sequence Spread Spectrum plus OFDM modulation to provide robust, interference-resistant solution in a multi-user environment
- Support of 64/128/256-bit WEP encryption and WPA (Wi-Fi Protected Access) high-level encryption
- Support of Ad-Hoc / Infrastructure mode
- Support of software AP function.
- Support of most popular operating systems including Windows 98SE/ME/2000/XP/Server 2003
- Plug-and -Play installation

1.2 Application

Infrastructure

The major difference between Infrastructure network and Ad-hoc wireless network is that the former requires an Access point. For old buildings, open areas, or frequently changing environments, just install the WL-U356 on your desktop or laptop, and thus you can get connected to the wired Ethernet through a wireless Access Point. SOHO users can then access the Internet and share all kinds of data with the other wired or wireless clients within the coverage of wireless signals. For enterprise users, the installation of multiple Access Points to enlarge the coverage of wireless

signals can provide wireless users with seamless network access.

The Infrastructure mode is appropriate for enterprise-scale wireless access to a central database or provides various wireless applications for mobile users.

Infrastructure mode also supports roaming capabilities for mobile users. More than one BSS can be configured as an Extended Service Set (ESS). The continuous wireless network connectivity allows users to roam freely within an ESS. All wireless clients using WL-U356 or other IEEE 802.11b compliant wireless adapters within one ESS must be configured with the same ESS ID and to use the same radio channel.

Before adopting an ESS with roaming capability, choosing an available radio channel with less interference is highly recommended. Proper Access Point positioning combined with a clear radio channel will greatly enhance performance.
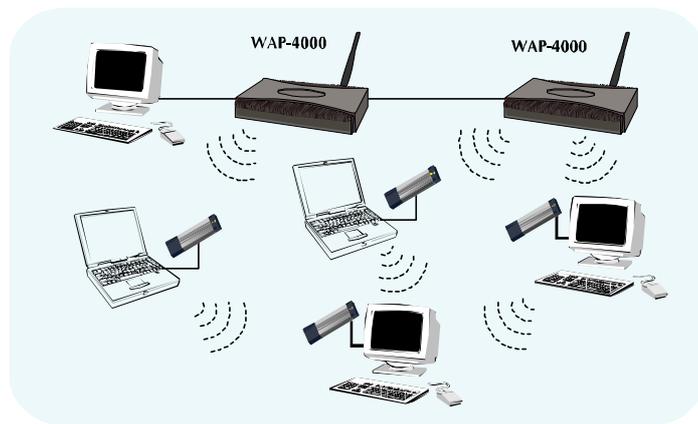
Ad-Hoc

Still complaining about the high price of wireless access points? This mode is the easiest and cost-effective way to meet your requirements. It enables you to construct wireless networking in no time without any access point.

Ad-hoc mode is a wireless network type in which a group of computers equipped with WL-U356 or other wireless adapters are connected together to form an independent wireless LAN. All computers operating in this mode must be configured to share the same radio channel.

In this scenario, new devices can be quickly added; however, wireless stations can only communicate with the other peers that belong to the same IBSS (Independent Basic Service Set).

Soft AP

This feature converts the wireless USB adapter into a wireless access point immediately, and you thus can create an instant wireless network, which spares the additional cost of purchasing a wireless access point. It makes WL-U356 a compact wireless access point with all basic functions contained in an ordinary access point.

General Application

WL-U356 offers a fast, reliable, cost-effective solution for wireless access to the various network scenarios:

1. Remote access to corporate network for information

E-mail, file transfer and terminal service.

2. Difficult-to-wire environments

Historical or old buildings, public occasions, venues and open area where it is difficult to wire.

3. Frequently changing environments

Factories, Retailers, and Offices that frequently change locations and rearrange the workplace

4. Temporary network access

Events, exhibitions, construction sites or some important occasions that require temporary network access.

5. Access to database for mobile workers

Doctors, nurses, retailers, white-collar workers who need access to database while roaming in the hospital, retail store or office.

6. SOHO (Small Office and Home Office) users

SOHO users who are in need of easy-to-install and wide coverage networking.

1.3 Specification

Product	54Mbps Wireless USB Adapter
Models	WL-U356
Attach Interface	USB 2.0 A-type connector
LED Indicator	Link/ACT
Operating Frequency / Channel	2.412~2.462GHz (FCC, Canada) / 11 Channels 2.412~2.4835GHz (Japan, TELEC) / 14 Channels 2.412~2.472GHz (Euro ETSI) / 13 Channels
RF Modulation	OFDM with BPSK, QPSK, 16QAM, 64QAM
RF Output Power	15dBm (Typical)
Data Rate	802.11b: 1, 2, 5.5, 11Mbps 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps auto-rate fall back
Media Access Protocol	CSMA/CA + ACK, IEEE802.11b Compliant
Antenna	Internal patch antenna
Range	Up to 300 feet outdoor and 100 feet indoor
Working Mode	Ad-Hoc, Infrastructure
Management	Built-in utility or Windows XP/Server 2003 Wireless Zero Configuration utility

STANDARDS COMPLIANCE	
Electromagnetic Compatibility	FCC, CE

1.4 Package Contents

Before installation, please check the items of your package. The package should include the following items:

- One Wireless USB Adapter
- One USB Cable
- One CD-Based software (Including the Configuration Utility, Driver and User's Manual)
- One Quick Installation Guide

If any of the above items is missing, contact your supplier as soon as possible.

1.5 Minimum System Requirements

Before installation, please check the following requirements with your equipment.

- Pentium Based (above) IBM-compatible PC system with one vacany USB 1.1/2.0 port
- CD-ROM drive
- Windows 98SE/2000/ME/XP/Server 2003 Operating System
- At least 5 MBytes of free disk space for utility and driver installation

1.6 Installation Considerations

- Beware of the walls and ceilings. Each wall or ceiling can reduce your wireless cover range form 3-90 feet. Properly position your Access Points, Residential Gateways, and computers so that the number of walls or ceilings residing between Access Points and clients is minimized.

- Building materials make a difference – A solid metal door or aluminum studs may have a negative effect on signal coverage range. Try to properly position Access Points and computers with wireless adapters so that there would be less obstacles existing between them.

- Keep your wireless LAN devices away from microwaves, cordless phones and child incubators. It is likely that the latter will cause interferences to the operation of your wireless LAN devices.

Chapter 2 Installation Procedure

Before you proceed with the installation, it is necessary that you have enough information about the Wireless USB Adapter. Follow the procedure described below in this chapter to install the USB adapter under Windows 98SE/ME/2000/XP/Server 2003.
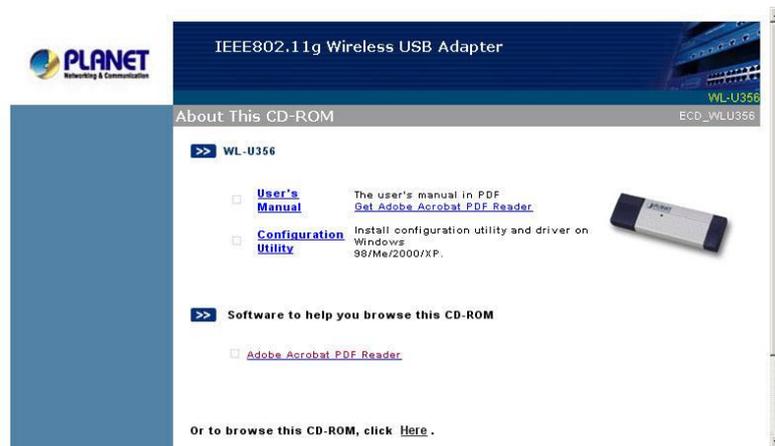
2.1 Configuration Utility Installation

The following installation operates under Window XP. The procedure also applies to Windows 98SE/ME/2000/Server 2003.

Note: If you had ever installed the other Wireless Cards before, please uninstall the existed drivers and utilities first.

A. Insert the bundled CD into the CD-ROM drive to launch the autorun program. Once completed, a menu screen will show up as follows.

B. Click the "Configuration Utility" hyperlink in the WL-U356 field to initiate the installation procedure. You will see the below InstallShield Wizard window. Please click "Next" to continue.
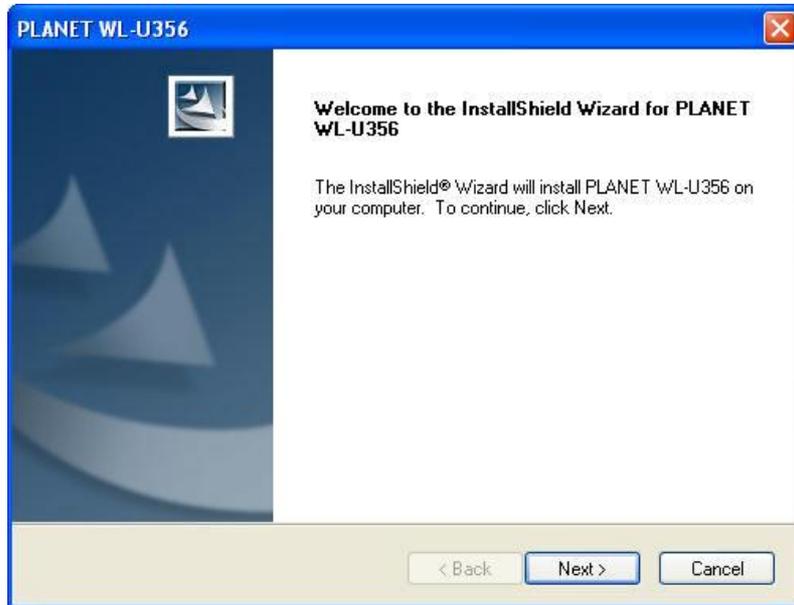
> **Note:** If the above screen does not appear, click "Start" at the taskbar. Then, select "Run" and type "E:\Utility\WL-U356\setup.exe", where E is your CD-ROM drive.

C. You may click "Browse" to specify the destination folder you prefer for the installation of utility. Otherwise, you can keep the default setting and click "Next" to proceed.

D. Once the utility is installed, select "Finish" to complete the installation procedure.
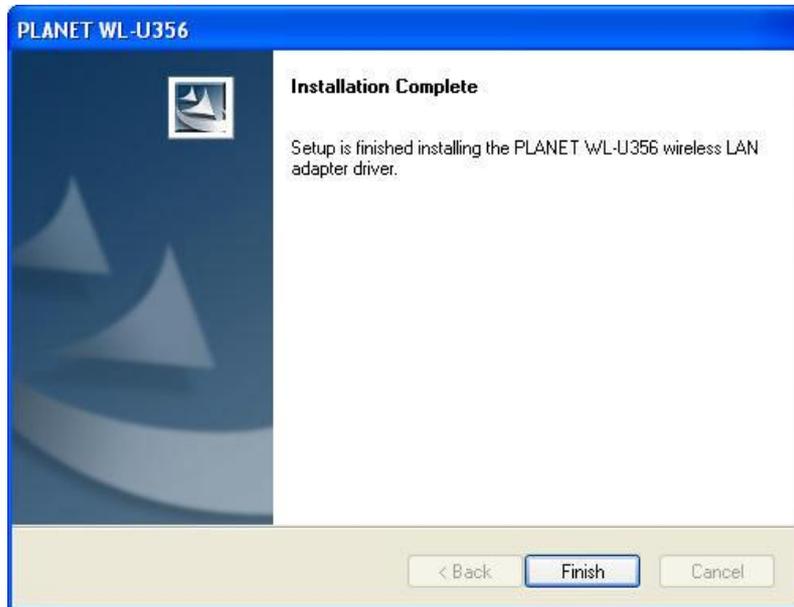
Note: If your operating system is Windows XP/Server 2003, the below window will pop up. Please select "Continue Anyway" to continue.

Note: If your operating system is Windows 2000, the below window will pop up. Please choose "Yes" to go on.

2.2 Driver Installation

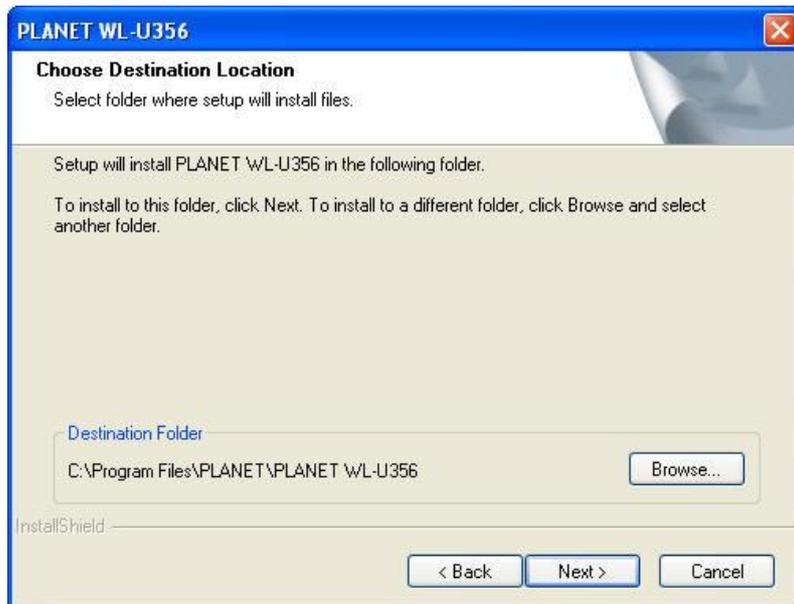**Note***:* The following installation operates under Windows XP. The procedure also applies to Windows Server 2003. If your operating system is Windows 2000, please directly skip to step 3. If your operating system is Windows 98SE, Windows will automatically detect and install the device and ask you to insert the system installation CD to complete the entire procedure. Just click "Yes" to continue.

A. Insert WL-U356 into a vacant USB port on the computer.

B. Windows will automatically detect the device. Choose "Install the software automatically (Recommended)". Then click "Next" to continue.

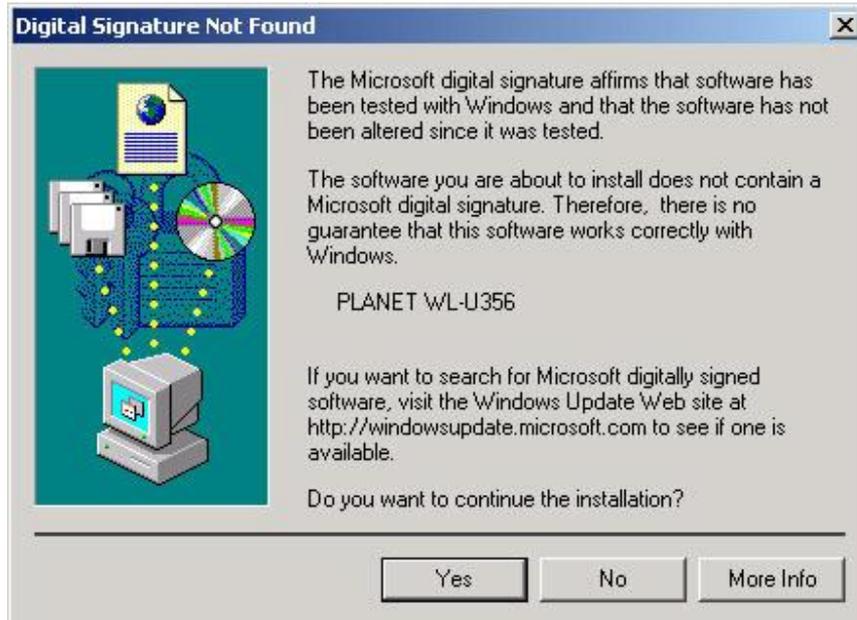**C.** A screen will appear to inform you that the USB adapter has not passed Windows Logo

testing (WHQL). Click "Continue Anyway" to proceed since the card has been tested thoroughly to verify the compatibility.

Note: If your operating system is Windows 2000, the below window will pop up. Please click "Yes" to continue.

D. When the driver is installed, click "Finish" to complete the installation procedure.

Chapter 3 Configuration Utility

The Configuration Utility is a powerful tool that helps you to configure WL-U356 easily and monitor the status of wireless communication. By double-clicking 🌐 in the system tray, the dialog box will appear as follows:

> **Note:** It is highly recommended that you use PLANET utility tool to configure WL-U356 rather than Windows XP/ Server 2003 Wireless Zero Configuration unless you prefer the latter. Windows Server 2003 Wireless Zero Configuration will take over the configuration of the USB adapter after installing the configuration utility and driver for the USB adapter. Make sure to disable the Wireless Zero Configuration utility provided by Windows Server 2003 before launching PLANET utility. To complete this, firstly, restart your computer, and click the Windows Server 2003 networking icon in the system tray, and then click "Advanced" in "Wireless Network Connection" window. Uncheck "Use Windows to configure my wireless network settings" and click "OK" to exit (If your operating system is Windows 98SE/ME/2000/XP, this step can be ignored). At last, double-click the utility icon 🌐 in the system tray to use the configuration utility. About the details please refer to the Quick Installation Guide.

Right-click the icon, there are some items for you to use the configuration utility:

◆   Open Utility Window: It enables you to open the configuration utility tool.

◆   Exit PLANET WL-U356: Select this to close the configuration utility tool.

3.1 Wireless Connection Status

When you open the configuration utility, the system will scan all the channels to locate all the access points and wireless stations within the signal coverage. Then it will automatically connect to the access point or wireless station with the strongest signal strength. This screen displays all the information about the current wireless connection.
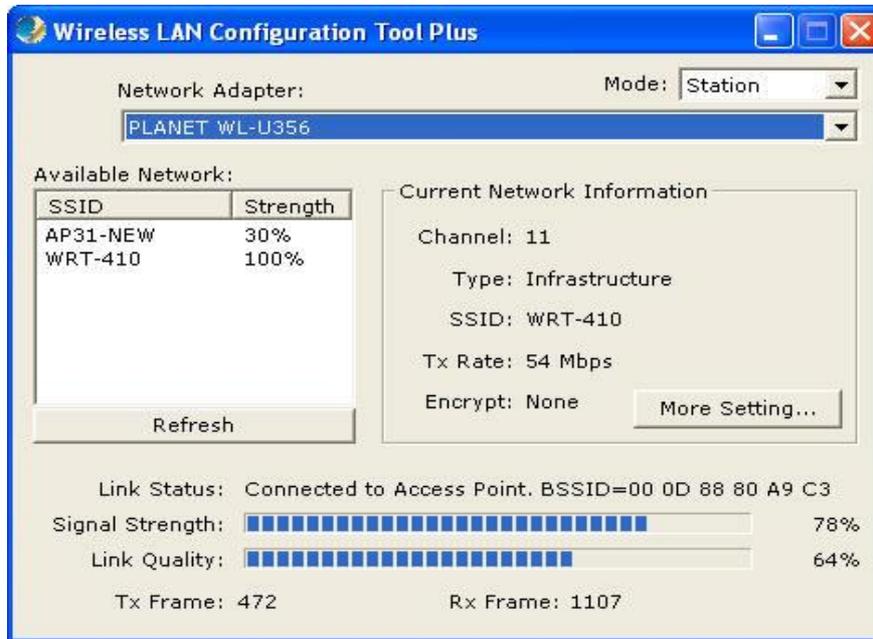
- ◆ **Mode:**
  - ➢ Station: Configure the USB adapter as a wireless station.
  - ➢ Access Point: Switch the USB adapter into a wireless access point.
- ◆ **Network Adapter:** Displays the product information of the USB adapter.
- ◆ **Available Network:** Displays all the SSID and Signal Strength of wireless access point and stations nearby. To rescan the available wireless networks, please click the "Refresh" button. The USB adapter can associate with the specified wireless access point or station on the list by double-clicking the station directly or selecting the preferred device, and then pressing the "Connect this site" button.
- ◆ **Current Network Information:** Displays the information about the wireless network which WL-U356 is connected to. The information includes Channel, Type, SSID, TX Rate and Encryption settings. Please refer to the section 3.2 for detailed descriptions of each item.
- ◆ **More Settings**: Press this button for further settings including disable/enable WEP Power Saving Mode, and so on. Please refer to the Section 3.2, 3.3 and 3.4 for detailed descriptions of each item.
- ◆ **Link Status**: Displays the status of the current wireless connection.
- ◆ **BSSID**: Shows the MAC address of the network (i.e. the connected Access Point) the USB adapter is linked to.
- ◆ **Signal Strength**: Indicates the signal strength level, which helps to find out the proper positioning of the wireless device for quality wireless communication.
- ◆ **Link Quality:** Indicates the quality of the active link.
- ◆ **TX/RX Frame**: Shows the number of valid transmitted/received data frames of the USB adapter.

3.2 More Setting…

You can enter this screen by clicking the "More Setting…" button. Here you can specify the wireless network to which WL-U351 intends to connect, enable/disable the WEP data encryption, save or load the settings into/from the profile, etc.

◆ **General Connection Setting:** Displays the information including Channel, SSID, Tx Rate and Network Type. You can click the "Change" button to modify these values.

➢ **Channel**: Shows the number of the radio channel used for the wireless networking. This parameter is not configurable in the Infrastructure mode.

➢ **Tx Rate**: Shows the Data Transfer Rate. There are Auto/1/2/5.5/11/6/9/12/18/24/36/48/54Mbps for selection. If the Auto Mode is selected, the device will choose the most suitable transmission rate automatically.

➢ **SSID**: Shows the SSID of the current associated wireless network.

➢ **Any**: If "Any" check box is enabled, WL-U356 will survey and connect to one of the available wireless networks without checking the consistency of the channel and SSID with the specified wireless device.

➢ **Network Type**:
Infrastructure: This mode requires the presence of an AP or Router to create a wireless network. All the communication is processed through the AP or Router.

Ad Hoc: This mode enables interconnecting of wireless adapters without the presence of an AP or Router.

➢ **Encryption:** There are four items for selection: Disable, WEP, TKIP, and AES. You can configure the encryption method based on the settings in the "Encryption Setting" field.

➢ **Authentication mode:**

Auto: Auto switching of the authentication mode depends on the one adopted on wireless network that the USB adapter is connected to.

Open system: In this mode, wireless stations directly associate with the access point without any authentication (null authentication). You can decide whether to employ WEP data encryption.

Shared key: In this mode, wireless stations communicate with the Access Point using the identical WEP key settings for authentication and data encryption. It always combines with WEP data encryption.

➢ **Change/Apply:** Click "Change" will enable you to configure the parameters in the "General Connection Setting" field. Meanwhile, it will turn into "Apply" for you to confirm the modified settings.

◆ **Encryption Setting:** You can enable/disable WEP and WPA encryption within the wireless network. Please refer to the Section 3.3 for detailed descriptions.

◆ **Profile:**

➢ **Profile Name:** You can save the network settings as a profile file by assigning it a name.

➢ **Load:** Load the settings from the specified profile file in the "Profile name" list. The new settings will take effect immediately.

➢ **Save Current:** Enter a profile name and click this to write the current settings to a profile file in the "Profile name" list.

➢ **Delete:** Delete the profile you have selected.

◆ **Other:**

➢ **Advanced Setting:** Click this for more advanced setting. Please refer to the Section 3.4 for detailed descriptions.

➢ **Information:** To view the basic information of WL-U356. Please refer to the Section 3.5 for detailed descriptions.

3.3 WEP and WPA Encryption
3.31 WEP Setting

WEP is both a data encryption method and an authentication mechanism, which ensures authenticated user access and secures data transfer on the wireless network. To implement WEP, the Authentication type and the WEP key format, length and ID must be identical on the AP and client side. WL-U356 supports 64/128/256-bit Hex/ASCII WEP encryption.
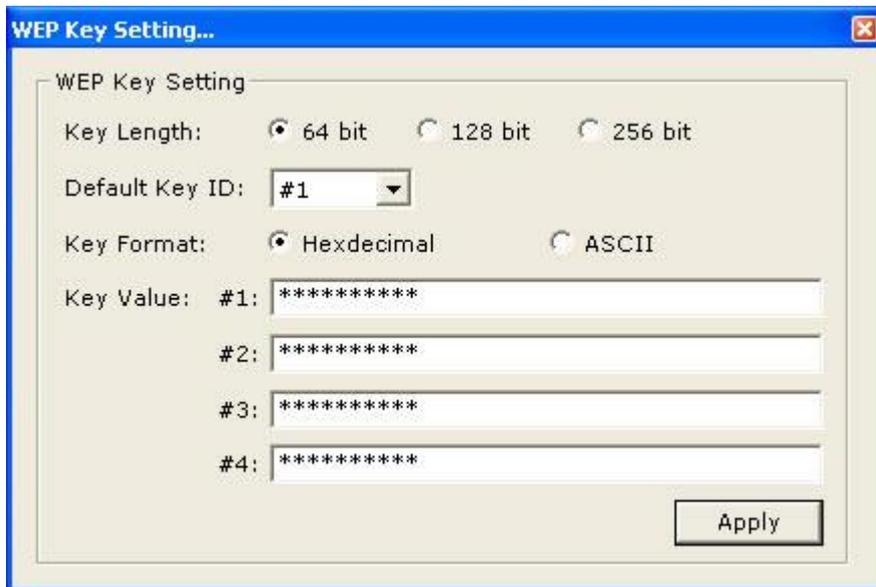
- ◆ **Key Length:** Select the 64, 128, or 256-bit WEP key to encrypt transmitted data. Larger key length will provide higher level of security, but the throughput will thus be affected.
- ◆ **Default Key ID:** Select one of the four keys (1~4) as the specified encryption key.
- ◆ **Key Format:**
  - ➢ **Hexdecimal:** Only "A-F", "a-f", and "0-9" are allowed to be entered.
  - ➢ **ASCII:** Digits, characters or signs are allowed to be entered. It's more recognizable for users.
- ◆ **Key Value**: The keys are used to encrypt data transmitted on the wireless network. Fill the text box by following the rules below:
  - ➢ **64-bit:** Enter 10-digit Hex values or 5-digit ASCII values as the encryption keys. For example: "0123456aef".
  - ➢ **128-bit:** Enter 26-digit Hex values or 13-digit ASCII values as the encryption keys. For example: "01234567890123456789abcdef"
  - ➢ **256-bit:** Enter 58-digit Hex values or 29-digit ASCII values as the encryption keys.
- ◆ **Change/Apply:** Click "Change" enables you to configure the WEP key. In the meantime, the button will change into "Apply" for you to confirm your new settings.

3.32 WPA Setting

In view of the defects of WEP encryption, WPA (Wi-Fi Protected Access) provides better security by adopting TKIP/AES encryption method and key rotation mechanism. There are two types of WPA mode: WPA-Radius and WPA-PSK. WPA-Radius is designed for enterprise use and requires a Radius server and a Certificate Authority (CA) for user authentication and data encryption, while WPA-PSK is designed for home and SMB users who do not have or cannot afford a Radius server and a Certificate Authority. To implement WPA, the WPA settings must be identical on the AP and the wireless station side.

- ◆ **Connection Information:**
  - ➢ **Protocol:** There are two kinds of protocols for WPA user authentication- TLS and PEAP. TLS and PEAP require a Radius server and the Certificate Authority. The main difference between the 2 protocols is TLS requires both the radius server's and the client's certificates, while PEAP requires only the server's certificate. Moreover, PEAP requires a set of user name of password, which are supposed to be preconfigured by the network administrator.
  - ➢ **User name:** It is the setting for PEAP protocol.
  - ➢ **Password:** It is the setting for PEAP protocol.
- ◆ **Pre-shared key:** It is used for WPA-PSK mode. Enter 8 to 63 characters in ASCII format to generate the password for authentication.
- ◆ **Certificate:** All available certificates for TLS or PEAP will be displayed in the list. Please select a proper one for user or server authentication.
- ◆ **WEP key:** If the AP uses WEP for user authentication or data encryption, please click "WEP KEY SETTING" to configure the WEP key.
- ◆ **Change/Apply:** Click "Change" to configure the WPA setting. In the meantime, the button

will change into "Apply" for you to confirm your new settings.

3.4 Advanced Setting

Here you can perform country roaming, enable/disable power saving mode, and configure the fragmentation threshold and RTS/CTS threshold of WL-U356.
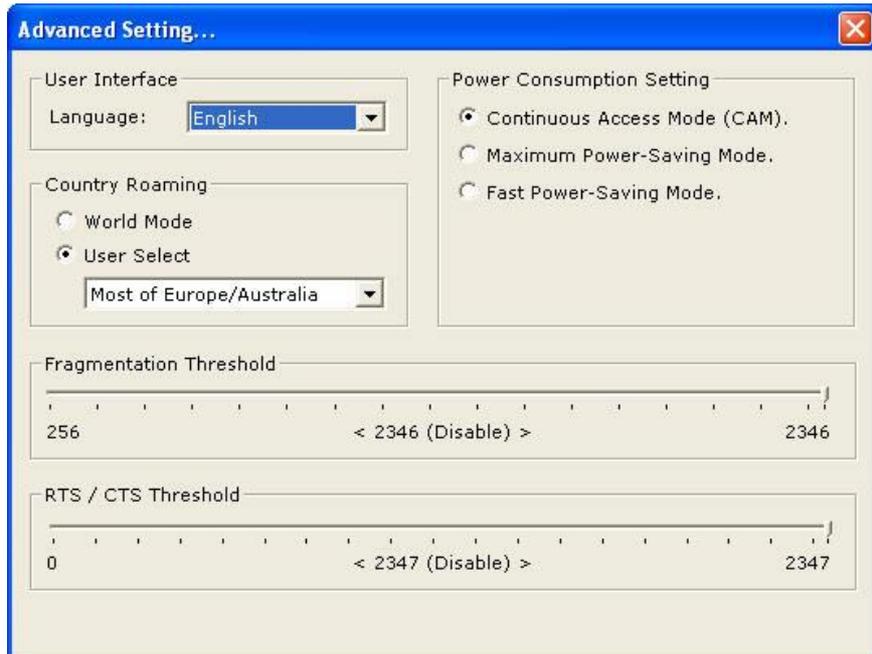
◆ **User Interface:** Select the display language of the utility. Two languages are available: English and Traditional Chinese.

◆ **Country Roaming:** This feature is developed based on IEEE 802.11d, which is a standard make wireless devices operate with the proper transmission power on the appropriate channel regulated by the country where users are located.

➢ **World Mode:** Select this to perform the country roaming and the adapter will follow the settings of the associated AP automatically.

➢ **User Select:** Users can select the country where they are located. The available channels will vary based on the selected country.

◆ **Power Consumption Setting:**

➢ **Continuous Access Mode (CAM):** The adapter will always stay in active mode. No power-saving function will be activated.

➢ **Maximum Power-Saving Mode:** Enable the power-saving function when the adapter is idle. This mode applies to PDA best because it saves most power. Its Implementation will cause additional overhead to your wireless network.

➢ **Fast Power-Saving mode:** This mode also provides the power-saving function, but the power consumption in this mode is higher than that of the "Maximum Power-Saving Mode". This mode applies to laptops. Its implementation will also cause additional overhead to your wireless network.

◆ **Fragmentation Threshold:** This value defines the maximum transmitted packet size.

Any packet size is larger than it will be fragmented. If you hit upon a high packet error rate, try to increase this value, but the performance will thus be affected. Keeping the default setting applies to most scenarios.

◆ **RTS/CTS Threshold**: This feature focuses on solving the "Hidden Note" issue and avoiding subsequent collisions. If you encounter a high packet error rate and high latency, try to adjust this value to find the suitable one for your wireless network. However, its implementation will cause additional overhead to your wireless network.
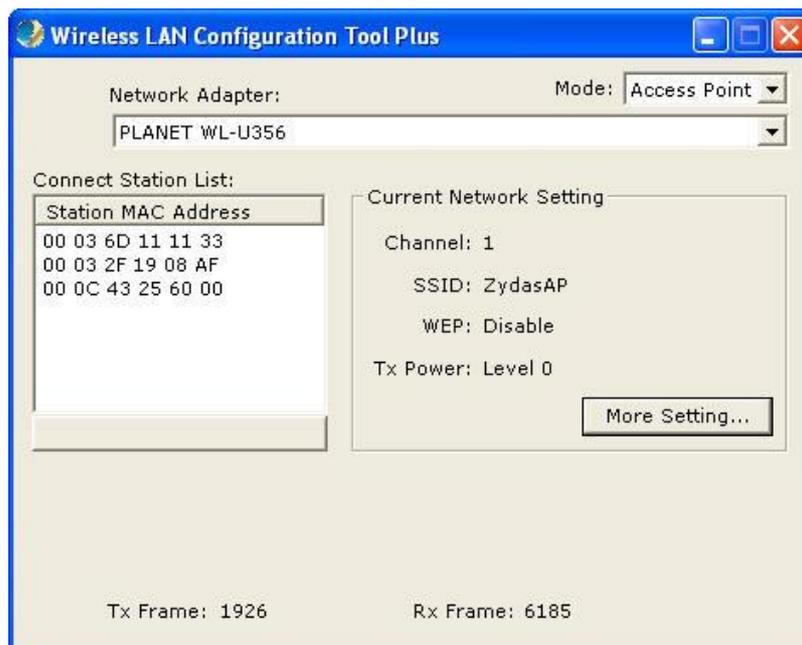
3.5 Information

This screen shows the current driver and utility version, and the MAC Address of the adapter.

3.6 Software AP mode

This mode turns the USB adapter into a wireless access point immediately. As an AP, it comes with all basic functions contained in an ordinary AP as follows:


◆ **Mode:** There are two modes available: Station and Access Point.
  ➢ **Station:** Set the USB adapter as a wireless client/station.
  ➢ **Access Point:** Switch the USB adapter into a wireless access point.
◆ **Network Adapter:** Display the product information of the USB adapter.

◆ **Connect Station List:** Display all the MAC addresses of the wireless stations associating with the AP.

◆ **Current Network Setting:** Displays the information about the current wireless network, including Channel, SSID, WEP and Tx Power Level.

◆ **More Setting:** Press this button for further settings including disable/enable WEP, MAC address Filter and Bridge Adapter, etc. Please refer to the Section 3.7 for detailed descriptions of each item.

◆ **Tx and Rx Frame:** Shows the number of valid transmitted/received data frames of the AP.

3.7 Access Point Setting

You can enter this screen by clicking the "More Setting…" button. Here you can configure the AP connection settings such as Channel, Basic Rate, SSID, Tx Power, WEP, Authentication Mode and other advanced functions.
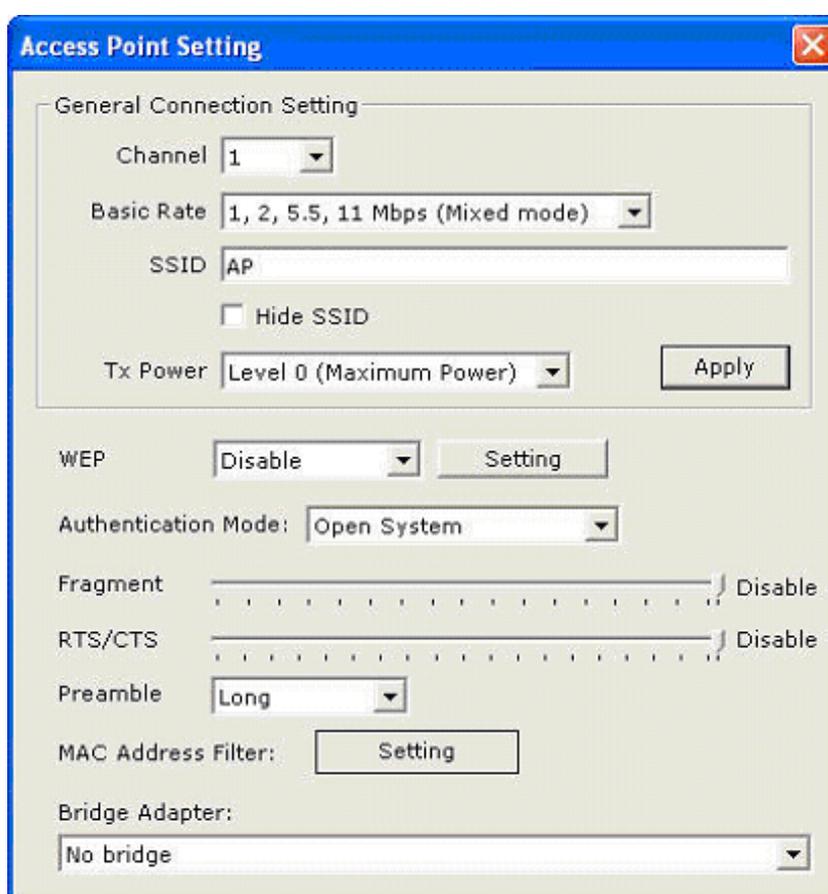
◆ General Connection Setting: Displays the connection information of the AP, including Channel, Basic Rate, SSID and Tx Power. You can click the "Change" button to modify these values.

 ➢ **Channel**: Selects the number of the radio channel used by the AP.

 ➢ **Basic Rate:** Selects the basic data transmission rate supported by the AP. There are four options, including "1, 2Mbps (Mixed mode)", "1, 2, 5.5, 11Mbps (Mixed)," 1, 2, 5.5, 11, 6, 12, 24Mbps (802.11g), and "6, 12, 24Mbps (802.11g only)." If the AP

works in 11b or 11b/g mixed mode, you can choose either "1, 2 Mbps" or "1, 2, 5.5, 11Mbps". If the AP operates in pure 11g mode, you can choose one of the four modes. But for better performance, the last two modes (1, 2, 5.5, 11, 6, 12, 24Mbps and 6, 12, 24 Mbps) are recommended.

➢ **SSID:** Service Set Identifier (up to 32 printable ASCII characters). The SSID must be identical for all the clients and AP of the same wireless network.

➢ **Hide SSID:** If this is checked, the AP will not incorporate its SSID into the field of the beacon frame regularly sent by the AP, which means only wireless stations set with the same SSID can connect to the AP. It prevents the AP from unauthorized user access.

➢ **Tx Power:** There are four levels (Level 0-3) for you to configure the transmission power of the AP. The higher transmission power, the larger transmission distance and wireless signal coverage will be.

➢ **Change/Apply:** Click "Change" will enable you to configure the parameters in the "General Connection Setting" field. Meanwhile, it will turn into "Apply" for you to confirm the modified settings.

◆ **WEP:** You can disable/enable the WEP encryption. To implement it, the Authentication type (Open system/Shared key) and the WEP key format (Hex/ASCII), length (64/128/256-bit) and ID(1-4) must be identical on the AP and client side. The AP supports 64/128/256-bit Hex/ASCII WEP encryption. About detailed descriptions, please refer to the Section 3.3.

◆ **Authentication Mode:**

➢ **Open system:** In this mode, wireless stations directly associate with the access point without any authentication (null authentication). You can decide whether to employ WEP data encryption.

➢ **Shared key:** In this mode, wireless stations communicate with the access point using the identical WEP key settings for user authentication and data encryption. It always combines with WEP data encryption.

◆ **Fragment:** This value defines the maximum transmitted packet size. Any packet size is larger than it will be fragmented. If you hit upon a high packet error rate, try to increase this value, but the performance will thus be affected. Keeping the default setting applies to most scenarios.

◆ **RTS/CTS:** This feature focuses on solving the "Hidden Note" issue and avoiding subsequent collisions. If you encounter a constant high packet error rate and high latency, try to adjust this value to find the suitable one for your wireless network. However, its implementation will cause additional overhead to your wireless network.

◆ **Preamble:** It defines the length of the CRC block for communication within the wireless network. There are two types available: Long and Short. If your wireless network consists

of 11b stations, use Long Preamble for better compatibility. Otherwise, Short Preamble will be a good choice in terms of the performance.

◆ **MAC Address Filter:** It enables the AP to control the network access by MAC address filtering of the wireless clients.
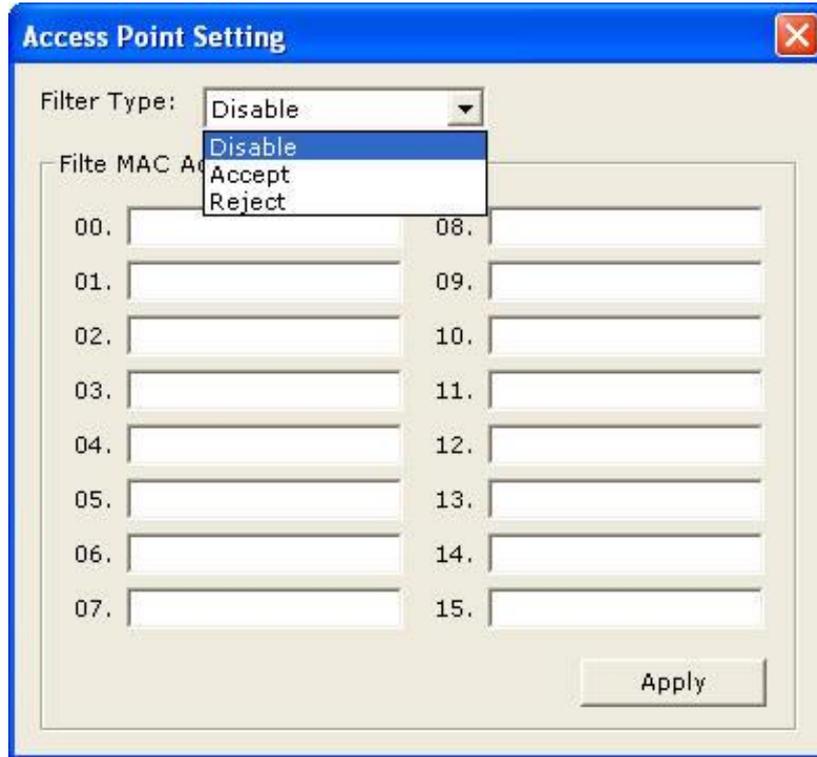
➢ **Filter Type**: There are three options- **Disable**, **Accept** and **Reject**. **Disable** makes you turn off the MAC address filter function. **Accept** means only wireless stations with the MAC addresses preconfigured on the below list will be granted access. **Reject** signifies only wireless stations with the MAC addresses preconfigured in the below list will be denied access. After finishing the setting, press the "Apply" button to make the new setting into effect.

➢ **Filter MAC Address:** The MAC address is a 12-digit hexadecimal value, a unique identification for network devices. There are fifteen sets of MAC address which can be preconfigured in each field of the list. Enter the MAC addresses of the wireless stations you want to grant or deny access by the AP.

◆ **Bridge Adapter:** The wireless stations connected to the AP can access the wired network through the bridge adapter. You can select the Ethernet adapter in the list as a bridge between the wireless and wired networks.

Chapter 4 Troubleshooting

This section provides solutions to problems usually encountered during the installation and operation of the USB adapter. Read the description below to diffuse your doubts.

What is the IEEE 802.11g standard?

802.11g is the latest IEEE standard for high-speed WLAN communications that provides up to 54Mbps data rate in the 2.4GHZ band. It has become the mainstream technology of current WLAN networks. It uses OFDM modulation to reach higher data transmission rate and backward compatible with 802.11b

What is the IEEE 802.11b standard?

The IEEE 802.11b WLAN standard subcommittee, which formulates a standard for the industry. The objective is to enable WLAN hardware from different manufacturers to interoperate.

What features does the IEEE 802.11 standard provide?

The product supports the following IEEE 802.11 functions:
- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What is Ad-hoc?

An Ad-hoc mode is a wireless network type in which a group of computers equipped with wireless adapters are connected as an independent wireless LAN without any access point. All computers operating in this mode must be configured to share the same radio channel and SSID.

What is Infrastructure?

The difference between Infrastructure network and Ad-hoc network is that the former requires an Access point. The Infrastructure mode is appropriate for enterprise-scale wireless access to a central database or provides various wireless applications for mobile users.

What is BSS ID?

An Infrastructure network is called a Basic Service Set (BSS). All the wireless stations in a BSS must share the same BSS ID.

What is TKIP?

It is another encryption method to overcome the inherent weaknesses of WEP, a next generation of WEP. It adopts new algorithm (Michael) to generate 128/192-bit encryption keys and provides per-packet key mixing, a message integrity check and a re-keying mechanism.

What is AES?

AES (Advanced Encryption Standard) is a chip-based encryption method of new generation and has been incorporated into the newly-approved security standard 802.11i. It supports 128, 192 and 256-bit encryption key length and adopts Rijndael algorithm. It is widely believed it is impossible to crack AES.

What is DSSS?   What is FHSS?   And what are their differences?

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitters and receivers. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the

23

military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).